Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
CSRIC V SS7 Security Best Practices	)	PS Docket No. 18-99
	)	
_____	)	

COMMENTS OF
SPRINT CORPORATION

Sprint Corporation ("Sprint") submits the following comments in response to the Federal Communication Commission's ("FCC" or "Commission") Public Safety and Homeland Security Bureau ("Bureau") Public Notice DA 18-333, issued April 3, 2018, which seeks public comment, including from communications service providers and other stakeholders, regarding the implementation and effectiveness of the March 2017 recommendations made by the Commission's fifth Communications Security, Reliability and Interoperability Council ("CSRIC V") to help mitigate potential Signaling System 7 ("SS7") security threats.[1]

I. The CSRIC V SS7 Security Best Practice Recommendations Were the Result of Significant Industry-Government Collaboration.

In response to heightened concerns regarding potential SS7 protocol security vulnerabilities, the Commission tasked CSRIC V Working Group 10 with assessing existing and

[1] Public Notice, *Public Safety and Homeland Security Bureau Requests Comment on Implementation of Signaling System 7 Security Best Practices*, DA 18-333, PS Docket No. 18-99, rel. April 3, 2018 ("Public Notice"). SS7 is a signaling protocol supporting call setup, routing, exchange, and billing functions in communications networks by sending messages between fixed and mobile communications service providers.

potential SS7 security risks and developing recommendations to help address those security challenges. Working Group 10 consisted of a broad range of representatives from both wireless and wireline service providers, equipment manufacturers, security solution providers and the U.S. Government (Department of Homeland Security ("DHS"), National Telecommunications and Information Administration ("NTIA")), among others. Sprint was pleased to participate in this important collaborative effort.

The Commission's CSRIC provided these expert representatives an opportunity to gather together within a single forum with laser-focus to review, analyze and identify a targeted set of recommendations designed to mitigate this potential threat. Working Group 10 first completed a Risk Assessment report that provided background on SS7 technology, potential targets, attack vectors and potential impacts.[2] Working Group 10 subsequently issued a separate Final Report, which outlined specific recommendations that industry could take to help reduce SS7 security risks, and identified areas of future CSRIC exploration and study.[3] CSRIC V voted to adopt those recommended best practices, which include the following:

1. Continue to implement signaling interconnection monitoring and filtering based on GSMA guidelines;
2. Utilize GSMA security best practices and guidelines to secure signaling interconnection;

[2] CSRIC V: Working Group 10, Legacy System Risk Reduction Working Group, Interim Report – Risk Assessment and Summary Public Report (December 2016).

[3] CSRIC V: Working Group 10, Legacy Systems Risk Reductions, Final Report (March 2017) ("CSRIC SS7 Report").

3. Engage signaling aggregators in their efforts to address overall security, monitoring and filtering;
4. Continue to leverage and expand existing threat information sharing resources;
5. Continue efforts regarding automated threat information sharing through the CTIA-sponsored information sharing pilot to advance telecommunications specific use cases;
6. Continue to participate in industry and standards forums and adopt the GSMA recommended controls to address emerging Diameter security risks;
7. Continue to explore further work as it relates to the possible benefits of circles-of-trust;
8. Continue efforts regarding ongoing security assessment of network signaling infrastructure to detect and mitigate possible threat vectors; and
9. Support the use of available encryption technologies for voice and data communications.[4]

In August 2017, the Bureau issued a public notice encouraging communications service providers to implement these best practices.[5] The Bureau now seeks comment on the progress industry has made in applying the recommendations, the factors considered in implementing them, and input on their effectiveness, among other things.[6]

---

[4] *Id.* at 18-19.

[5] Public Notice, *FCC's Public Safety and Homeland Security Bureau Encourages Implementation of CSRIC Signaling System 7 Security Best Practices*, DA 17-799, rel. Aug. 24, 2017.

[6] *See* Public Notice at 2.

II. The CSRIC SS7 Security Best Practice Recommendations Provide Effective Guidance to Help Mitigate Potential SS7 Security Threats.

Security is of paramount importance to Sprint. Sprint invests tremendous resources to support the various activities necessary to secure its network operations against present and emerging security threats. Sprint also participates in a number of communications sector organizations formed to strengthen and enhance the nation's broader security profile.

SS7 security is an essential element of Sprint's overall network security program. Utilizing a proactive, "defense in depth" approach, Sprint has implemented multiple layers of security to protect its network, including its SS7 network, from malicious activity. Sprint's SS7 security framework takes advantage of not only Code Division Multiple Access ("CDMA") technology, which manages SS7 signals differently than other technologies, but also Sprint's unique network architecture and network security practices. These mechanisms help protect Sprint's network to ensure a high level of network performance and to safeguard customer traffic.

Sprint has implemented the recommendations as applicable to its network technology. Indeed, CSRIC V's SS7 recommendations validated Sprint's internal practices and confirmed that its external engagement activities helped strengthen protective efforts on an industry-wide basis.

The Bureau seeks comment on the factors that may have been considered in implementing the recommendations.[7] Of note, a few of the CSRIC V SS7 guidelines

---

[7] *Id.*

recommend that industry implement GSMA best practices, which apply specifically to GSM (Global System for Mobile communications) network operations in the SS7 context.[8] Because Sprint's relevant network operates using CDMA, rather than GSM, technology, not all of the GSMA-related SS7 best practices can be implemented on Sprint's network. Where technically feasible, however, Sprint has implemented the SS7 best practices outlined in GSMA's FS.11 and other guidelines for relevant GSM-originated traffic. Furthermore, Sprint has addressed the security issues that those guidelines seek to tackle in a way that is tailored to its CDMA technology, network architecture, and network security practices.

Overall, Sprint has found that CSRIC V's SS7 security recommendations are a valuable resource supporting the industry-wide effort to mitigate the SS7 security threat. In Sprint's experience, the monitoring and filtering practices are particularly effective in directly countering and reducing potential exploits. At the same time, the recommendations take a holistic approach, not only promoting network-specific protective measures, but also encouraging increased awareness and ongoing exploratory work. Indeed, Sprint has observed that the recommendations have helped increase awareness of the SS7 security issue throughout all levels of industry and have focused attention on timely, actionable measures that can be taken to address the matter. In addition, CSRIC's forward-looking recommendations will help maintain momentum supporting efforts that assess any new emerging signaling security issues.

As part of its ongoing commitment to security, Sprint will continue to review and enhance its SS7 security posture to keep pace with the evolving threat landscape. Sprint will

[8] *See e.g.,* CSRIC SS7 Report at 11.

also collaborate with industry and government to identify, assess and address any new SS7 security vulnerabilities that may arise as well as any next generation signaling security challenges. [9]

III. Conclusion

Sprint thanks the Bureau for the opportunity to participate in this effort to enhance SS7 security and looks forward to continued participation and collaboration on security matters within CSRIC.

Respectfully submitted,

SPRINT CORPORATION

/s/ Charles W. McKee
Charles W. McKee
Vice President, Government Affairs
Federal & State Regulatory

Maria L. Cattafesta
Senior Counsel, Government Affairs

Sprint Corporation
900 7th Street, N.W., Suite 700
Washington, D.C. 20001
703-433-3786

May 3, 2018

[9] For example, Sprint participated in CSRIC VI's Working Group 3 to review, assess and recommend best practices and approaches to address potential Diameter security threats.